UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,607	06/28/2001	Neil S. Fishman	13768.164	5110

7590 05/19/2005	EXAMINER
RICK D. NYDEGGER	CERVETTI, DAVID GARCIA

WORKMAN, NYDEGGER & SEELEY
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/894,607	FISHMAN ET AL.
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>28 June 2001</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-14 and 16-34</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-14 and 16-34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>28 June 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>1/10/03, 6/28/01</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Applicant's arguments filed February 28, 2005, have been fully considered but

they are not persuasive.

Response to Amendment

Examiner approves the amendment to the specification received on February 28,

2005. The objection to the drawings is withdrawn. The objection to the specification is

withdrawn.

Cohen et al. disclose a single sign-on mechanism, where the access information

preferably is centralized in the PKM, thus acting as a gateway (column 5, lines 1-6).

Furthermore, Cohen et al. also disclose a system that maps user related information to

the targets that user may have access. These target information includes password,

username, and domain. This information is used to logon to the target systems. The

logon coordinator substitutes given data received from the PKM into substitution

variables in the invocation strings returned from the CIM (column 7, lines 1-20). The

PKM database, is acting as a gateway, remotely interposed between a remote client

and a content server (target) and mapping the authentication credentials received from

the remote client. Cohen et al. also disclose that the PKM may be local or remote

(column 6, lines 46-59).

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

Claim 16 recites the limitation " a method as recited in claim 15" in line 1 of the

claim. There is insufficient antecedent basis for this limitation in the claim. Examiner

has treated claim 16 as reciting the limitation "a method as recited in claim 12".

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5.   **Claims 1-7, 24-30 are rejected under 35 U.S.C. 102(a) as being anticipated**

by Cohen et al. (US Patent Number: 6,178,511).

Regarding claim 1, Cohen et al. teach in a computerized system that includes

one or more clients accessing a gateway and content server that are part of a network,

wherein access to the content server requires authentication credentials, the network

maintaining gateway authentication credentials that specify one or more access

privileges tailored to access through the gateway, a method of authenticating a client

comprising a gateway performing the acts of: defining an authentication filter in a

gateway that is remotely interposed between a remote client and a content server,

wherein the authentication filter maps authentication credentials received from the

remote clients according to pre-established criteria, the authentication filter including a

domain identifier and a username modifier (column 2, lines 33-42, column 6, lines 46-

59); receiving authentication credentials at the gateway from the remote client that

include both a domain and a user name corresponding to access permissions for

accessing the resources at the content server through the domain (column 6, lines 29-

37); mapping the received authentication credentials based on the pre-established

criteria, and by changing at least one of the domain and user name received from the

remote client to different domain or user name, respectively, wherein the domain

identifier is configured to change the domain and wherein the username modifier is

configured to change the user name (column 6, lines 1-67); and sending the mapped

authentication credentials to the network, and such that the client's access to the

content source is based on the mapped authentication credentials comprising the at

least one of a changed user name and a changed domain (column 6, lines 38-45).

Regarding claim 2, Cohen et al. teach wherein gateway authentication

credentials and other authentication credentials are maintained in separate domains,

and wherein the act of mapping the received authentication credentials includes

changing a domain name that is part of the received authentication credentials (column

6, lines 1-67, column 7, lines 1-20, figure 8).

Regarding claim 3, Cohen et al. teach wherein the act of mapping the received

authentication credentials includes replacing the domain name that is part of the

received authentication credentials with another domain name (column 6, lines 1-67,

column 7, lines 1-20, figure 8).

Regarding claim 4, Cohen et al. teach wherein the gateway authentication

credentials are maintained in a credential database that is administered separately from

domain authentication credentials and recognized by the content server only in

authenticating client access through the gateway (column 4, lines 60-65, column 5, lines

30-45).

Regarding claim 5, Cohen et al. teach wherein gateway authentication

credentials and other authentication credentials share a common domain, and wherein

the act of mapping the received authentication credentials includes changing a

username that is part of the received authentication credentials (column 5, lines 30-45,

column 6, lines 1-67).

Regarding claim 6, Cohen et al. teach wherein the act of mapping the received

authentication credentials includes adding a suffix to the username (column 5, lines 30-

45).

Regarding claim 7, Cohen et al. teach wherein the act of mapping the received

authentication credentials includes adding a prefix to the username (column 5, lines 30-

45).

Regarding claim 24, Cohen et al. teach in a computerized system that includes

one or more mobile clients accessing a mobile gateway and content server that are part

of a network, wherein access to the content server requires authentication credentials

that may contain a combination of numbers, upper case letters, lower case letters, and

punctuation, and wherein at least some of the mobile clients use relatively short

authentication credentials or have an input system that is optimized for numeric input

rather than for letters or punctuation, the network maintaining mobile authentication

credentials that specify one or more access privileges tailored to mobile client access, a

computer program product that implements a method of authenticating a mobile client,

comprising: a computer readable medium for carrying machine executable instructions

for implementing the method (column 15, lines 34-58); and wherein said method is

comprised of machine-executable instructions for a mobile gateway performing the acts

of (column 15, lines 34-58): defining an authentication filter in a gateway that is remotely

interposed between a remote client and a content server, wherein the authentication

filter maps authentication credentials received from the remote clients according to pre-

established criteria, the authentication filter including a domain identifier and a

username modifier (column 2, lines 33-42, column 6, lines 46-59); receiving

authentication credentials at the gateway from the remote client that include both a

domain and a user name corresponding to access permissions for accessing the

resources at the content server through the domain (column 6, lines 29-37); mapping

the received authentication credential, based on the pre-established criteria, and by

changing at least one of the domain and user name received from the remote client to

different domain or user name, respectively, wherein the domain identifier is configured

to change the domain and wherein the user name modifier is configured to change the

user name (column 6, lines 1-67); and sending the mapped authentication credentials to the network, and such that the client's access to the content source is based on the mapped authentication credentials comprising the at least one of a changed user name and a changed domain (column 6, lines 38-45).

Regarding claim 25, Cohen et al. teach a computer program product as recited in claim 24 wherein mobile authentication credentials and other authentication credentials are maintained in separate domains and wherein the act of mapping the received authentication credentials includes changing a domain name that is part of the received authentication credentials (column 6, lines 1-67, column 7, lines 1-20, figure 8).

Regarding claim 26, Cohen et al. teach a computer program product as recited in claim 25 wherein the act of mapping the received authentication credentials includes replacing the domain name that is part of the received authentication credentials with another domain name (column 6, lines 1-67, column 7, lines 11-17).

Regarding claim 27, Cohen et al. teach a computer program product as recited in claim 24 wherein the mobile authentication credentials are maintained in a credential database that is administered separately from domain authentication credentials and recognized by the content server only in authenticating mobile clients (column 4, lines 60-65, column 5, lines 30-45).

Regarding claim 28, Cohen et al. teach a computer program product as recited in claim 24 wherein mobile authentication credentials and other authentication credentials share a common domain, and wherein the act of mapping the received authentication

credentials include changing a username that is part of the received authentication credentials (column 5, lines 30-45).

Regarding claim 29, Cohen et al. teach a computer program product as recited in claim 28 wherein the act of mapping the received authentication credentials includes adding a suffix to the user-name (column 5, lines 30-45, column 6, lines 1-67).

Regarding claim 30, Cohen et al. teach a computer program product as recited in claim 28 wherein the act of mapping the received authentication credentials includes adding a prefix to the username (column 5, lines 30-45, column 6, lines 1-67).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 8, 12-14, 16-19, 22-23, and 34 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Cohen et al., and further in view of Puhl et al. (US Patent

Number: 6,223,291).

Regarding claim 8, Cohen et al. do not disclose expressly wherein the client

includes one or more identified wireless application protocol servers providing gateway

and content server access to one or more other clients, the method further comprising

the act of accepting authentication credentials only from the one or more identified

wireless application protocol servers. However, Puhl et al. teach wherein the client

includes one or more identified wireless application protocol servers providing gateway

and content server access to one or more other clients (column 9, lines 21-28), the

method further comprising the act of accepting authentication credentials only from the

one or more identified wireless application protocol servers (column 6, lines 40-55,

figure 1). Therefore, it would have been obvious to one having ordinary skill in the art at

the time the invention was made to use Cohen et al. system on a wireless network. One

of ordinary skill in the art would have been motivated to do so to provide access to

resources from a mobile client (Puhl et al., column 1, lines 5-55).

Regarding claim 12, Cohen et al. teach in a computerized system that includes

one or more mobile clients accessing a mobile gateway and content server that are part

of a network, wherein access to the content server requires authentication credentials

that may contain a combination of numbers, upper case letters, lower case letters, and

punctuation, and wherein at least some of the mobile clients use relatively short

authentication credentials or have an input system that is optimized for numeric input

rather than for letters or punctuation, the network maintaining mobile authentication

credentials that specify one or more access privileges tailored to mobile client access, a

method of authenticating a mobile client comprising a mobile gateway performing steps

for: altering, at a gateway, authentication credentials that include a user name and a

domain to produce mapped authentication credentials that match mobile authentication

credentials maintained on the network by at least one of changing the domain name

and the user name, wherein changing the user name includes one of adding characters

to the user name and substituting only a portion of the user name (column 2, lines 33-

42, column 6, lines 1-67); identifying a mobile client to the network using the altered

authentication credentials (column 6, lines 38-45); and accessing content provided by

the network in accordance with the access privileges allowed by the mobile

authentication credentials (column 6, lines 1-67). Cohen et al. do not disclose expressly

that a WAP server may be used. However, Puhl et al. teach a WAP server

communicating with one or more remote mobile clients (figure 1). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was

made to use Cohen et al. system on a wireless network. One of ordinary skill in the art

would have been motivated to do so to provide access to resources from a mobile client (Puhl et al., column 1, lines 5-55).

Regarding claim 13, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein the step for altering authentication credentials comprises the acts of: defining an authentication filter that maps authentication credentials received from mobile clients according to pre-established criteria (column 2, lines 33-42, column 6, lines 1-67); and mapping the received authentication credentials based on the pre-established criteria (column 6, lines 19-37).

Regarding claim 14, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein the step for identifying a mobile client comprises the acts of: receiving authentication credentials from a mobile client (column 6, lines 29-37); and sending mapped authentication credentials to the network, wherein the mobile client's access to the content source is determined from the mapped authentication credentials (column 6, lines 38-45).

Regarding claim 16, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein changing at least one of the domain name and a username includes either adding a suffix to the username or replacing the domain name with another domain name (column 5, lines 30-45, column 6, lines 1-67, column 7, lines 1-20).

Regarding claim 17, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein the mobile authentication credentials are maintained in a credential database that is administered separately from domain authentication credentials and recognized by the content server only in authenticating mobile clients (column 4, lines 60-65, column 5, lines 30-45).

Regarding claim 18, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein mobile authentication credentials and other authentication credentials share a common domain (column 5, lines 30-45).

Regarding claim 19, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Puhl et al. teach wherein the mobile client includes one or more identified wireless application protocol servers providing mobile gateway and content server access to one or more other mobile clients (column 9, lines 21-28), the step for identifying a mobile client comprising the act of accepting authentication credentials only from the one or more identified wireless application protocol servers (column 6, lines 40-55).

Regarding claim 22, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 12 above. Furthermore, Cohen et al. teach wherein a trust relationship exists between the mobile authentication credentials and other authentication credentials with respect to one or more access privileges (column 6, lines 19-67).

Regarding claim 23, the combination of Cohen et al. and Puhl et al. teaches the limitations as set forth under claim 22 above. Furthermore, Cohen et al. teach wherein the one or more access privileges included within the trust relationship that exists between the mobile authentication credentials and the other authentication credentials comprise a delegate access permission (column 5, lines 15-67, column 6, lines 1-18).

Regarding claim 34, Cohen et al. do not disclose expressly a computer program product as recited in claim 24 wherein the mobile client includes one or more identified wireless application protocol servers providing mobile gateway and content server access to one or more other mobile clients, the method further comprising computer-executable instructions for performing the act of accepting authentication credentials only from the one or more identified wireless application protocol servers. However, Puhl et al. teach a computer program product as recited in claim 24 wherein the mobile client includes one or more identified wireless application protocol servers providing mobile gateway and content server access to one or more other mobile clients (column 9, lines 21-28), the method further comprising computer-executable instructions for performing the act of accepting authentication credentials only from the one or more identified wireless application protocol servers (column 6, lines 40-55, figure 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use Cohen et al. system on a wireless network. One of ordinary skill in the art would have been motivated to do so to provide access to resources from a mobile client (Puhl et al., column 1, lines 5-55).

8.   Claims 9-11, 31-33 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Cohen et al., and further in view of Starkovich et al. (US Patent

Number: 6,715,080).

Regarding claim 9, Cohen et al. teach the limitations as set forth under claim 1

above. Cohen et al. teach wherein the gateway authentication credentials correspond to

other authentication credentials that allow access to a content server, and wherein a

trust relationship exists between the gateway authentication credentials and other

authentication credentials with respect to one or more access privileges (column 6, lines

19-67). However, Cohen et al. do not disclose expressly the acts of: receiving a request

for content available at the content server; sending the request to the network; receiving

the requested content from the network; and sending the received content to the client.

Starkovich et al. teach the acts of: receiving a request for content available at the

content server; sending the request to the network; receiving the requested content

from the network; and sending the received content to the client (figure 1, column 6,

lines 15-67, column 7, lines 1-32). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to receive a request for

content available at a content server; send a request to the network; receive the

requested content from the network; and send the received content to the client. One of

ordinary skill in the art would have been motivated to do so because it was well known

in the art to send requests for content to a server, receive the content, and return the

content to the requesting client (Starkovich et al., column 2, lines 1-64).

Regarding claim 10, the combination of Cohen et al. and Starkovich et al.

teaches the limitations as set forth under claim 9 above. Furthermore, Cohen et al.

teach wherein the content available at the content server comprises email content

(column 2, lines 28-41, column 4, lines 22-35).

Regarding claim 11, the combination of Cohen et al. and Starkovich et al.

teaches the limitations as set forth under claim 9 above. Furthermore, Cohen et al.

teach wherein the one or more access privileges included within the trust relationship

that exists between the gateway authentication credentials and the other authentication

credentials comprise a delegate access permission (column 5, lines 15-67, column 6,

lines 1-18).

Regarding claim 31, Cohen et al. teach the limitations as set forth under claim 24

above. Cohen et al. teach a computer program product as recited in claim 24 wherein

the mobile authentication credentials correspond to other authentication credentials that

allow access to a content server, and wherein a trust relationship exists between the

mobile authentication credentials and other authentication credentials with respect to

one or more access privileges (column 6, lines 19-67). However, Cohen et al. do not

disclose expressly the method further comprising computer-executable instructions for

performing the acts of: receiving a request for content available at the content server;

sending the request to the network; receiving the requested content from the network;

and sending the received content to the mobile client. Starkovich et al. teach the

method further comprising computer-executable instructions for performing the acts of:

receiving a request for content available at the content server; sending the request to

the network; receiving the requested content from the network; and sending the

received content to the mobile client (figure 1, column 6, lines 15-67, column 7, lines 1-

32). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to receive a request for content available at a content

server; send a request to the network; receive the requested content from the network;

and send the received content to the client. One of ordinary skill in the art would have

been motivated to do so because it was well known in the art to send requests for

content to a server, receive the content, and return the content to the requesting client

(Starkovich et al., column 2, lines 1-64).

Regarding claim 32, the combination of Cohen et al. and Starkovich et al.

teaches the limitations as set forth under claim 31 above. Furthermore, Cohen et al.

teach a computer program product as recited in claim 31 wherein the content available

at the content server comprises email content (column 2, lines 28-41, column 4, lines

22-35).

Regarding claim 33, the combination of Cohen et al. and Starkovich et al.

teaches the limitations as set forth under claim 31 above. Furthermore, Cohen et al.

teach a computer program product as recited in claim 31 wherein the one or more

access privileges included within the trust relationship that exists between the mobile

authentication credentials and the other authentication credentials comprise a delegate

access permission (column 5, lines 15-67, column 6, lines 1-18).

9.   **Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable**

over Cohen et al. and Puhl et al. as applied to claim 12 above, and further in view

of Starkovich et al.

Regarding claim 20, the combination of Cohen et al. and Puhl et al. teaches the

limitations as set forth under claim 12 above. Cohen et al. do not disclose expressly

wherein the step for accessing content provided by the content server comprises the

acts of: receiving a request to access content from the mobile client; sending the

request to the network; receiving the requested content from the network; and sending

the received content to the mobile client. Starkovich et al. teach the acts of: receiving a

request to access content from the mobile client; sending the request to the network;

receiving the requested content from the network; and sending the received content to

the mobile client (figure 1, column 6, lines 15-67, column 7, lines 1-32). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention

was made to receive a request to access content from the mobile client; send a request

to the network; receive the requested content from the network; and send the received

content to the mobile client. One of ordinary skill in the art would have been motivated

to do so because it was well known in the art to send requests for content to a server,

receive the content, and return the content to the requesting client (Starkovich et al.,

column 2, lines 1-64).

Regarding claim 21, the combination of Cohen et al., Puhl et al, and Starkovich

et al. teaches the limitations as set forth under claim 20 above. Furthermore, Cohen et

al. teach wherein the content is email content (column 2, lines 28-41, column 4, lines

22-35).

Conclusion

10.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100